



## デスクトップ マネジメントについて

hpワークステーションxw4000  
hpワークステーションxw6000

製品番号 : 301201-291

2002年10月

このガイドでは、一部のモデルにプリインストールされているセキュリティ機能とインテリジェント マネジメント機能の概念および使用手順について説明します。

© 2002 Hewlett-Packard Company  
© 2002 日本ヒューレット・パッカード株式会社

Microsoft、MS-DOS、Windows、およびWindows NTは、米国Microsoft Corporationの米国およびその他の国における登録商標です。

Intel、Pentium、Intel Inside、およびCeleronは、米国Intel Corporationの米国およびその他の国における登録商標です。

その他、本書に掲載されている会社名、製品名はそれぞれ各社の商標または登録商標です。

本書の内容につきましては万全を期しておりますが、本書の技術的あるいは校正上の誤り、省略に対して、また本書の適用の結果生じた間接損害を含めいかなる損害についても、責任を負いかねますのでご了承ください。本書の内容は、現状有姿のままで提供されるもので、商品性または特定目的への適合性に関する黙示の保証などを含むいかなる保証も含みません。本書の内容は、将来予告なしに変更されることがあります。HP製品に対する保証は、当該製品に付属の限定的保証規定に明示的に記載されているものに限られます。本書のいかなる内容も、当該保証に新たに保証を追加するものではありません。

本書には、著作権によって保護された所有権に関する情報が掲載されています。本書のいかなる部分も、Hewlett-Packard Companyの書面による承諾なしに複写、複製、あるいは他言語へ翻訳することはできません。

本製品は、日本国内で使用するための仕様になっており、日本国外で 사용되는場合は、仕様の変更を必要とすることがあります。

本書に記載されている製品情報は、日本国内で販売されていないものも含まれている場合があります。



---

**警告：**その指示に従わないと、人体への傷害や生命の危険を引き起こす恐れがあるという警告事項を表します。

---



---

**注意：**その指示に従わないと、装置の損傷やデータの損失を引き起こす恐れがあるという注意事項を表します。

---

#### デスクトップ マネジメントについて

hpワークステーションxw4000

hpワークステーションxw6000

初版 2002年10月

製品番号：301201-291

日本ヒューレット・パッカード株式会社

---

# 目次

## デスクトップ マネジメント

出荷時設定の変更	2
リモート システム インストール	3
ソフトウェアのアップデートと管理	3
Altiris eXpress	4
Altiris eXpress PC Transplant Pro	6
Altiris eXpress HP/Compaq Client Manager	6
System Software Manager	7
Product Change Notification (製品変更通知)	7
ActiveUpdate	8
ROMフラッシュ機能	8
リモートROMフラッシュ機能	9
ブート ブロックROM	9
リブリーク セットアップ機能	11
デュアル ステート電源ボタンの設定	12
省電力機能 (タイムアウトの設定)	13
インターネットの弊社ホームページ	13
標準規格およびパートナー企業	14
デスクトップ マネジメント インタフェース (DMI)	14
Wired for Management	15
資産情報管理機能およびセキュリティ機能	15
パスワードのセキュリティ	19
ネットワーク サーバ モード	24
ドライブロック	25
スマート カバー センサ/カバー リムーバブル センサ (Cover Removable Sensor)	28
スマート カバー ロック (Smart Cover Lock)	29
マスタ ブート レコード セキュリティ (Master Boot Record Security)	31
ケーブル ロック の取り付け	35
指紋認証テクノロジー	35
障害通知および復旧機能	35
ドライブ保護システム	36
Ultra ATA監視機能	36
耐サージ機能付連続供給電源装置	36
温度センサ機能	36

## 索引



---

# デスクトップ マネジメント

HPはデスクトップ マネジメントのパイオニアとして1995年に、デスクトップを完全に管理できる業界初のパーソナル コンピュータを世に送り出しました。以来、デスクトップ、ワークステーション、およびノートブック コンピュータの効果的な導入、設定、および管理に必要な標準化とインフラストラクチャの開発において業界全体の取り組みをリードしてきました。HPのインテリジェント マネジメント機能は、ネットワーク環境にあるデスクトップ、ワークステーション、およびノートブック コンピュータの管理と制御の分野で、標準のソリューションを提供しています。HPは、業界トップ クラスの管理ソフトウェア ソリューション提供企業との提携関係により、これらの企業の製品とインテリジェント マネジメント機能の互換性を確保しています。インテリジェント マネジメント機能は、ライフサイクル ソリューションを提供する幅広い取り組みの中でも重要な位置を占めるもので、デスクトップ コンピュータのライフサイクルの4つの側面である計画、導入、管理、移行でユーザをサポートします。

このガイドでは、デスクトップ マネジメント機能の7つの主要な機能と特長について説明します。

- 出荷時設定の変更
- リモート システム インストール
- ソフトウェア アップデートおよびマネジメント機能
- ROMフラッシュ
- 標準規格およびパートナー企業
- 資産情報管理機能およびセキュリティ機能
- 障害通知および復旧機能



このガイドで説明される機能のサポートについては、機種またはソフトウェアのバージョンにより異なることがあります。

---

## 出荷時設定の変更

お使いのコンピュータには、システム ソフトウェア イメージがプリインストールされています。ソフトウェアの設定手順を簡単に済ませると、すぐにコンピュータを使用できます。

プリインストールされたソフトウェア イメージの代りにカスタマイズされたシステム ソフトウェアおよびアプリケーション ソフトウェアを使うこともできます。カスタマイズされたソフトウェア イメージを展開するには、いくつかの方法があります。

- プリインストールされたソフトウェアを展開した後、追加するアプリケーションをインストールする。
- Altiris社のeXpress、Microsoft®社のMS Batch、またはMicrosoft社のNTDS (NT Distribution Share) などのソフトウェアの導入用ツールを使用して、プリインストール ソフトウェアの代りにカスタマイズされたソフトウェア イメージを使用する。
- ディスク複製手順を使用して、ハードディスク ドライブの内容を別のハードディスクにコピーする。

最適なコンピュータ環境の構築方法は、ご使用になる情報技術内容や作業内容によって異なります。ソリューションおよびサービスに関する弊社のホームページ (<http://www.compaq.com/solutions/pcsolutions/>、英語サイト) には、ご使用の環境に適したコンピュータの導入方法を選択する際に役立つ情報が掲載されています。ここからMicrosoftまたはPXEベースの導入用ツールを組み込むためのガイドやユーティリティをダウンロードできます。

コンパック リストア CD (またはRestore Plus! CD)、ROMからのセットアップ、およびACPI対応ハードウェアにより、システム ソフトウェアのリストア、コンフィギュレーション マネジメント機能、トラブルシューティング、および省電力機能を利用することができます。

## リモート システム インストール

リモート システム インストールを使用すれば、ネットワーク サーバからソフトウェアやコンフィギュレーション情報（コンピュータの設定情報）を取り出して、コンピュータを起動したりセットアップすることができます。リモート システム インストールの機能は、通常システム セットアップを行ったり、コンフィギュレーション ツールとして使用しますが、次のような場合にも使用することができます。

- 1台以上の新しいコンピュータにソフトウェア イメージを導入するとき
- ハードディスク ドライブをフォーマットするとき
- アプリケーションやドライバをインストールするとき
- オペレーティング システム、アプリケーション ソフトウェア、またはドライバをアップデートするとき

リモート システム インストールを起動するには、起動時に表示される画面でHPのロゴの右下に[F12 = Network Service Boot]と表示されたら、すぐに[F12]キーを押します。画面のメッセージに従って、リモート システム インストールを起動します。

リモート システム インストールは、お使いの機種によりサポートされない場合があります。

HPとAltiris社の提携により、企業におけるコンピュータの導入と管理を短時間で容易に実行できるツールが開発されました。このツールを使用すると、TCO（維持管理費）が大幅に削減されます。HPのコンピュータが、企業環境内で最も管理しやすいクライアント マシンになります。

## ソフトウェアのアップデートと管理

HPでは、デスクトップ コンピュータおよびワークステーションのソフトウェアを管理し、アップデートするためのツール（Altiris eXpress、Altiris eXpress PC Transplant Pro、Altiris eXpress HP/Compaq Client Manager、System Software Manager、Product Change Notification（製品変更通知）、およびActiveUpdate）を提供しています。

## Altiris eXpress

HPはAltirisとの連携を強め、コンピュータ業界をリードするソリューションを提供しています。これらのソリューションにより、デスクトップ コンピュータ、ノートブック コンピュータ、ハンドヘルド製品、およびサーバのライフサイクル全体を通じて、ハードウェアとソフトウェアの管理の複雑さが軽減されます。Altiris eXpressのインタフェースは、Windows®エクスプローラのように使いやすいので、システム管理者はカスタマイズされた企業標準ソフトウェア イメージを作成し、それをネットワーク上の1台または複数のクライアント マシンに速やかに導入できます。Altiris eXpressは、Intel社のWired for ManagementおよびPreboot Execution Environment (PXE)をサポートします。Altiris eXpressとHPのコンピュータのリモートシステム インストール機能を利用すれば、システム管理者は、ソフトウェア イメージを導入するために新しいコンピュータの設置場所まで行く手間を省くことができます。

Altiris eXpressのソリューションによって、既存のプロセスの自動化や、ユーザのIT環境において発生する問題への対処を効率的かつ効果的に行うことができます。Altiris eXpressのWebベースのインフラストラクチャを使用すれば、時間や場所を問わず、お使いのiPAQ Pocket PCからでも、システムの管理が可能になります。

Altiris eXpressのソリューションはモジュール化されているため、ワークグループの要件に応じて企業レベルに拡張できます。また、その他のクライアント管理ツールと統合し、Microsoft BackOffice/SMSに拡張機能を提供します。

Altiris eXpressの拡張されたソリューションは、次に示すITの4つの主要分野に主眼を置いています。

- 配備と移行
- ソフトウェアおよび操作の管理
- 資産管理
- ヘルプデスクと問題解決



Altiris eXpressでは、個別のブート ディスケットを使用せずに、オペレーティング システム、アプリケーション ソフトウェア、およびAltiris eXpress クライアントを含むディスク イメージを数分でインストールできます。Altiris eXpressを使用するとネットワーク管理者では以下の作業を行うことができます。

- 新規イメージを作成したり、既存のイメージを変更したりできます。または、ネットワーク上に、基準となるイメージがインストールされたコンピュータを複製することができます。
- 多様なワークグループ用にカスタマイズされたディスク イメージをいくつでも作成できます。
- イメージファイルを初めから作成するのではなく、編集して変更することができます。Altiris eXpressでは、NTFS、FAT16、またはFAT32など、システムに合わせたフォーマットでファイルが保存されているため、このことが可能です。
- 新しいコンピュータがネットワークに追加されるときに自動的に実行されるスクリプト（New PC Event）を作成できます。このスクリプトで、コンピュータのハードドライブのフォーマット、ROM BIOS のフラッシュ、標準ソフトウェア イメージ全体のインストールなどが実行できます。
- コンピュータ グループで実行するイベントのスケジュールを作成できます。

Altiris eXpressには、使いやすいソフトウェア配布機能も含まれています。Altiris eXpressを使用して、中央管理コンソールからオペレーティング システムとアプリケーション ソフトウェアをアップデートできます。System Software Managerと組み合わせてAltiris eXpressを使用すると、ROM BIOSとデバイス ドライバのソフトウェアもアップデートできます。

詳しくは、<http://www.compaq.com/easydeploy/index.html>（英語サイト）を参照してください。

## Altiris eXpress PC Transplant Pro

Altiris eXpress PC Transplant Proを使用すると、既存の設定、ユーザ設定、およびデータを保存し、新しい環境に迅速かつ簡単に移行することができます。アップグレードは何日も何時間もおかからず分単位で済み、移行後のデスクトップとアプリケーションは、外観も動きもユーザの期待どおりになります。

詳細情報および30日間試用版のダウンロード方法については、  
<http://www.compaq.com/easydeploy/index.html> (英語サイト) を参照してください。

## Altiris eXpress HP/Compaq Client Manager

Altiris eXpress HP/Compaq Client ManagerはAltiris eXpress内でHPのインテリジェント マネジメント機能を強力に統合し、HPのアクセス デバイスに以下のような優れたハードウェア管理機能を提供します。

- 資産管理用のハードウェア インベントリの詳細表示
- コンピュータの状態検査の監視および診断
- ハードウェア環境の変化についての事前通知
- マシン温度についての警告、メモリ異常の警告など、企業活動における重大な状況についての、Webサイトを利用した報告
- システム ソフトウェア (デバイス ドライバやROM BIOSなど) のリモート アップデート

Altiris eXpress HP/Compaq Client Managerについて詳しくは、  
<http://www.compaq.com/easydeploy/index.html> (英語サイト) を参照してください。

## System Software Manager

System Software Manager (SSM) は、複数のシステムにおいてシステム レベルのソフトウェアを同時にアップデートできるユーティリティです。SSMは、コンピュータのクライアントシステムで使用すると、ハードウェアおよびソフトウェアのバージョンを検出し、ファイル格納ディレクトリと呼ばれる中央のリポジトリから適切なソフトウェアをアップデートします。SSMでサポートされるドライバのバージョンは、ドライバのダウンロードサイトおよびサポート ソフトウェアCDに、独自のアイコンで示されています。ユーティリティのダウンロードまたはSSMについて詳しくは、<http://www.compaq.com/im/ssmwp.html> (英語サイト) を参照してください。

## Product Change Notification (製品変更通知)

PCN (Product Change Notification、製品変更通知) はHPの製品変更通知プログラムであり、ユーザにより作成されるカスタム プロファイルを保存する安全性の高いWeb サイトを利用して、以下のことを事前にかつ自動的に行います。

- ほとんどの企業向けコンピュータおよびサーバでハードウェアおよびソフトウェアの変更があった場合に電子メールでの通知を受け取る
- ほとんどの企業向けコンピュータおよびサーバについての Customer Advisoriesを含んだ電子メールを受け取る

PCNのWeb サイトでも、ほとんどの企業向けコンピュータおよびサーバについての製品変更通知およびCustomer Advisoriesを検索することができます。

PCNおよびカスタム プロファイルの作成方法について詳しくは、<http://www.compaq.com/pcn> (英語サイト) を参照してください。

## ActiveUpdate

ActiveUpdateはHPのクライアントベースのアプリケーションです。ActiveUpdateクライアントはユーザのローカル システムで稼動し、ユーザ定義のプロファイルを使用して、ほとんどの企業向けコンパック /HP コンピュータおよびサーバに関連するソフトウェアのアップデート版を事前にかつ自動的にダウンロードします。

ActiveUpdate、アプリケーションのダウンロード、およびカスタム プロファイルの作成方法について詳しくは、<http://www.compaq.com/activeupdate>（英語サイト）を参照してください。

## ROMフラッシュ機能

お使いのコンピュータでは、オペレーティング システムとの情報のやりとりなどを行う基本入出力システム（BIOS）が再プログラム可能なフラッシュ ROMに記憶されているので、必要に応じて簡単にアップグレードすることができます。ROMのアップグレードには RomPaq ディスケットが必要です。RomPaq ディスケットは、インターネットの弊社ホームページからダウンロードできます。ROMのアップグレード手順については、RomPaq ディスケットに付属の説明を参照してください。



**注意：**コンピュータにセットアップ パスワードを設定しておけば、システム ROMの内容が不用意に変更されるのを防ぐことができます。コンピュータにセットアップ パスワードが設定されていないと、ROMへの書き込みが禁止されていないので、不用意にROMの内容が変更されてしまう危険があります。

システムROMのバージョンがお使いのコンピュータのモデルやオペレーティング システムに合っていないと、コンピュータが正しく動作しないことがあります。

System Software Managerを使用すると、システム管理者が、複数のコンピュータに同時にセットアップ パスワードを設定することができます。

詳しくは、<http://www.compaq.com/im/ssmwp.html>（英語サイト）を参照してください。

---

## リモートROMフラッシュ機能

リモートROMフラッシュ機能を利用すれば、システム管理者は、ネットワーク管理端末からリモートでコンピュータのROMを安全に書き換えることができます。複数のHPのコンピュータに対してこのような作業をリモートで行うことができるので、ネットワーク上のコンピュータのROMを適切にアップグレードし、少ない費用で管理することができます。



リモートROMフラッシュを使用するには、リモート ウェイク アップ機能を使って、お使いのコンピュータの電源を入れておくか、再起動しておく必要があります。

リモートROMフラッシュについて詳しくは、<http://www.compaq.com/easydeploy> (英語サイト) でAltiris eXpress HP/Compaq Client ManagerまたはSystem Software Managerについての説明を参照してください。

## ブート ブロックROM

ブート ブロックROMが装備されているので、システムROMのアップグレード中に電源の障害が発生するなどしてROMの書き換えに失敗した場合も、システムROMを復旧またはアップグレードすることができます。ブートブロックはROMフラッシュの際にも更新されない領域に収められており、コンピュータの電源が入れられるたびにシステムROMフラッシュをチェックし、以下のいずれかの方法でコンピュータを起動します。

- システム ROM が有効な場合は、コンピュータは通常の方法で起動します。
- システムROMが有効でない場合は、システムROMの復旧作業を実行できるように、RomPaqディスクからのコンピュータの起動を、ブートブロックROMがサポートします。

ブートブロックROMはシステムROMが有効でないことを検出すると、"ピーピピ"とビーブ音を鳴らし、キーボード上の3つのランプを2回点滅させます。ブートブロックのリカバリ モードのメッセージが、画面に表示されます (一部のモデルのみ)。

ブートブロックのリカバリ モードになったら、次のように操作して、システムROMを復旧（アップグレード）してください。

1. ディスケット ドライブからディスクを取り出し、コンピュータの電源を切ります。
2. RomPaqディスクをディスク ドライブに挿入します。
3. コンピュータの電源を入れます。
4. RomPaqディスクが認識されない場合、RomPaqディスクを挿入してコンピュータを再起動するように指示されます。
5. セットアップ パスワードが設定されている場合、Caps Lock ランプが点灯し、パスワード入力を求められます。
6. セットアップ パスワードを入力します。
7. RomPaqディスクからの再起動が正しく行われ、システムROMの復旧またはアップグレードが正常に完了すると、キーボード上の3つのランプが点灯し、ビープ音が鳴ります。

ROMフラッシュに成功したことを確認するには、以下の手順に従います。

1. 有効なRomPaqディスクをディスク ドライブに挿入します。
2. システムの電源を切ります。
3. 再び電源を入れてROMを再フラッシュします。
4. ROMフラッシュが完了すると、3つのキーボード ランプがすべて点灯し、ビープ音が鳴ります。
5. ディスケットを取り出して電源を切ります。再び電源を入れてコンピュータを再起動します。

キーボード上の3つのランプが点灯しない場合は、次の表に従って、対処してください。

#### ブート ブロックROMによるキーボード ランプの状態

ブート ブロック モード	ランプの色	ランプの状態	意味
Num Lock	緑色	ON	RomPaq ディスケットが挿入されていないか、壊れているか、またはドライブが正常に動作していない
Caps Lock	緑色	ON	パスワードを入力してください
Num、Caps、 Scroll Lock	緑色	2回の点滅 (同時に"ピーピー"というビープ音)	ROMフラッシュに失敗した
Num、Caps、 Scroll Lock	緑色	ON	ブート ブロックROMフラッシュが完了した。コンピュータの電源を入れなおして、コンピュータを再起動してください



診断ランプは、USBキーボードでは点滅しません。

## リプリケート セットアップ機能

リプリケート セットアップ機能を使用すれば、コンピュータの設定情報（コンフィギュレーション情報）を他の同じモデルのコンピュータにコピーすることができます。この機能によって、複数のコンピュータに同じ設定を行う時間を短縮することができます。

次の手順で、リプリケート セットアップ機能を使って、コンピュータの設定情報を他のコンピュータにコピーします。

1. **[コンピュータ セットアップ ユーティリティ (F10)]**メニューを開きます。
2. **[ファイル] (File) → [ディスクットに保存] (Save to Diskette)** の順に選択したあと、画面上のメッセージに従って操作します。



この手順を行うには、内蔵ディスクット ドライブまたは外付け用ディスクット ドライブが必要です。

3. コンフィギュレーション情報をコピーするには、**[ファイル] (File) → [システム構成の復元] (Restore from Diskette)** の順に選択したあと、画面上のメッセージに従って操作します。

## デュアル ステート電源ボタンの設定

お使いのコンピュータでWindows 98、Windows 2000、Windows Me、またはWindows XPのACPI（Advanced Configuration and Power Interface）を使用している場合は、電源ボタンをコンピュータのON/OFFとしての機能のほか、サスペンドモードを起動するためのボタンとして設定することができます。サスペンドモードでは、電源を完全に切らずに、コンピュータの消費電力を低い状態に保つことができます。使用中のアプリケーションを終了せずに作業を途中で中断したい場合など、サスペンドモードに設定しておくことでコンピュータの電力を低く抑えることができます。

次の手順で電源ボタンのコンフィギュレーションを設定することができます。

1. Windows 2000の場合：[スタート]ボタンを左クリックし、[設定]→[コントロール パネル]→[電源オプション]の順に選択します。

Windows XPの場合：[スタート]ボタンを左クリックし、[コントロール パネル]→[パフォーマンスとメンテナンス]→[電源オプション]の順に選択します。

2. [電源オプションのプロパティ]で、[詳細]（Windows 2000の場合）または[詳細設定]（Windows XPの場合）タブを選択します。
3. [電源ボタン]で、電源ボタンの設定を選択します。

電源ボタンをサスペンドモードに設定している場合は、コンピュータの電源が入っているときに電源ボタンを押すと、直ちにサスペンドモードを起動することができます。サスペンドモードから復帰する際も、電源ボタンを押します。

電源ボタンをサスペンドモードに設定している場合にコンピュータの電源を切るには、電源ボタンを4秒以上押し続けます。



## 省電力機能（タイムアウトの設定）

Windows 98、Windows 2000、Windows Me、およびWindows XPでAdvanced Configuration and Power Interface（ACPI）を有効にした場合、ハードディスクドライブやモニタのスタンバイ モードを起動するまでのタイムアウトは、オペレーティング システムで有効、無効、またはカスタマイズできます。

1. Windows 2000の場合：[スタート]ボタンを左クリックし、[設定]→[コントロール パネル]→[電源オプション]の順に選択します。

Windows XPの場合：[スタート]ボタンを左クリックし、[コントロール パネル]→[パフォーマンスとメンテナンス]→[電源オプション]の順に選択します。

2. [電源オプションのプロパティ]で、[電源設定]タブを選択します。
3. 目的の電源設定を選択します。

## インターネットの弊社ホームページ

HPの技術者がHP製および他社製のソフトウェアのテストおよび修正を行い、オペレーティング システムに特化したサポート ソフトウェアを開発しました。このため、HPのコンピュータは非常に優れた性能、互換性、信頼性を兼ね備えています。

別の種類のオペレーティング システムをインストールしたり新しいバージョンのオペレーティング システムに移行する場合、それぞれのオペレーティング システム用に設計されたサポート ソフトウェアを実行してください。お使いのコンピュータにインストールされているバージョンと異なるバージョンのMicrosoft Windowsを実行したい場合、対応するデバイス ドライバおよびユーティリティをインストールして、すべての機能がサポートされ、正しく動作することを確認してください。

HPでは、快適な環境で、効率的にコンピュータをお使いいただくために、最新のデバイス ドライバ、ユーティリティ、フラッシュ ROMイメージなどを収録したサポート ソフトウェアを提供しています。サポートソフトウェアはインターネットの弊社ホームページ（<http://www.compaq.com>/または<http://www.compaq.co.jp/>）からダウンロードできます。

弊社のホームページには、HP 製のコンピュータで Microsoft Windows のオペレーティング システムを使用する際に必要な最新のデバイス ドライバ、ユーティリティ、フラッシュ ROM イメージなどが用意されています。

## 標準規格およびパートナー企業

HP のインテリジェント マネジメント機能は、DMI 2.0、Web-Based Enterprise Management、Intel の Wired for Management (WfM) 構想、SNMP および PXE (preboot execution environment) テクノロジなどのコンピュータ業界の標準に準拠しています。HP は、Microsoft、Intel、およびその他の主要企業と連携して、HP の製品に各社のマネージメント ソリューションを取り入れ、パーソナル システムに最新のインテリジェント マネジメント機能を提供しています。詳しくは、<http://www.compaq.com/easydeploy> (英語サイト) を参照してください。

## デスクトップ マネジメント インタフェース (DMI)

Desktop Management Task Force (DMTF) は、1992年に創設されたシステム管理の標準化を目指す業界団体であり、コンピュータの設定情報(コンフィギュレーション情報)へのアクセス方式の標準化のために Desktop Management Interface (DMI) の枠組みを定めました。HP は、DMTF の運営委員会および専門委員会のメンバーとして、DMI 規格に準拠するハードウェアおよびソフトウェアを開発しています。

DMI ソフトウェアについて詳しくは、「リモート マネージメント管理者ガイド」のヘルプ ファイルを参照してください。

## Wired for Management

Intel社のWired for Management構想は、Intel社のアーキテクチャをベースにしたシステムで、柔軟性やパフォーマンスを損なわずに管理費を削減することに主眼を置いています。Wired for Managementガイドラインは、インテリジェント マネジメント機能にデスクトップ製品の標準管理機能を提供する基本的なビルディング ブロックのガイドラインを提示しています。ただし、HPはこれだけにとどまらず、新しい機能をインテリジェント マネジメント機能に追加することにより、ネットワーク コンピューティング環境を管理するための広範なソリューションを提供しています。

必要なWired for Managementテクノロジーには、次のものが含まれます。

- デスクトップ マネジメント インタフェース (DMI) 2.0
- リモート システム インストール
- リモート ウェイクアップおよびリモート シャットダウン
- ACPI対応ハードウェア
- SMBIOS
- PXEのサポート

## 資産情報管理機能およびセキュリティ機能

HPのコンピュータに搭載される資産情報管理機能を使用すれば、HP Insight マネージャ製品やマネジメント ソリューション パートナー企業が提供するネットワーク管理ソフトウェアを使用して管理される資産情報を確認することができます。資産情報管理機能とこれらの管理ソフトウェア製品を統合することにより、お使いの環境に最適な管理ソフトウェアを選択することができます。今までご使用になっていたソフトウェアをより有効に活用することができます。

HP製のコンピュータは、ハードウェアとファームウェアに必要なDMI 2.0に準拠しています。

さらに、HPでは、コンピュータとデータを不正なアクセスから保護するために、リモートセキュリティ マネージメント機能や、その他のセキュリティ機能を備えています。

一部のモデルに装備されているスマート カバー センサ/カバー リムーバブル センサ (Cover Removable Sensor) およびスマート カバー ロック (Smart Cover Lock) のようなセキュリティ機能は、コンピュータの内部装置への不正なアクセスの防止に役立ちます。パラレル ポート、シリアル ポート、またはUSB ポートを無効にすることにより、あるいはリムーバブル メディア ブート機能を無効にすることにより、貴重な資産であるデータを保護できます。これ以外にも、メモリ脱着センサおよびスマート カバー センサ/カバー リムーバブル センサからの警告が自動的にHP Insight マネージャ製品に送信されることで、コンピュータの内部装置への不正なアクセスを防ぐことができます。




---

スマート カバー センサ/カバー リムーバブル センサおよびスマート カバー ロックは、一部のシステムにオプションとして装備されています。

---

次のユーティリティを使用して、セキュリティ機能の設定を管理できます。


- コンピュータ セットアップ ユーティリティ (Computer Setup Utilities) を使用してローカルで管理します。コンピュータ セットアップ ユーティリティの詳しい情報と手順については、コンピュータに付属の『コンピュータ セットアップ (F10) ユーティリティ ガイド』を参照してください。
- System Software Managerを使用してリモートで管理します。このソフトウェアにより、簡単なコマンドライン ユーティリティを使用して、ネットワークのセキュリティ機能の設定を確実に、一貫して集中管理することができます。

次の表と各項で、コンピュータ セットアップ ユーティリティ (F10) を使ってローカルでコンピュータのセキュリティ機能を管理する方法を説明します。

## セキュリティ機能

機能	目的	設定方法の概要
リムーバブル メディアからの起動 (Removable Media Boot) 制御	リムーバブル メディア ドライブからの起動を禁止する	コンピュータ セットアップ ユーティリティ (Computer Setup Utilities (F10)) メニューを使う
シリアル ポート (Serial Port)、パラレル ポート (Parallel Port)、USB ポート (USB Port)、赤外線インターフェイス コントロール (Infrared Interface Control) 制御	内蔵シリアル ポート、内蔵パラレル ポート、USB ポート、および、オプションの外部赤外線トランシーバを使ったデータ転送を禁止する	コンピュータ セットアップ ユーティリティ (F10) メニューを使う
電源投入時パスワード (Power-On Password)	電源投入時および再起動時に、パスワードを入力するまでコンピュータを使用禁止にする	コンピュータ セットアップ ユーティリティ (F10) メニューを使う
セットアップ パスワード (Setup Password)	パスワードを入力するまでコンピュータ セットアップ ユーティリティを使ったコンピュータの設定の変更を禁止する	コンピュータ セットアップ ユーティリティ (F10) メニューを使う
ネットワーク サーバ モード (Network Server Mode)	サーバとして使用するコンピュータに独自のセキュリティ機能を提供する	コンピュータ セットアップ ユーティリティ (F10) メニューを使う
ドライブロック (DriveLock)	特定のハードディスク ドライブにあるデータへの不正アクセスを禁止する (一部のモデルのみ)	コンピュータ セットアップ ユーティリティ (F10) メニューを使う
スマート カバー センサ/カバー リムーバブル センサ (Cover Removable Sensor)	コンピュータ本体のカバーが取り外されたことを知らせる。カバーを取り外した後はセットアップ パスワードを入力するまでコンピュータを使用できないように設定することもできる。この機能について詳しくは、Documentation Library CD に収録されている『ハードウェア リファレンス ガイド』を参照	コンピュータ セットアップ ユーティリティ (F10) メニューを使う

## セキュリティ機能（続き）

機能	目的	設定方法の概要
マスタ ブート レコード セキュリティ (Master Boot Record Security)	現在の起動可能ディスクのマスタ ブート レコードを誤って変更したり、不正に変更できないようにする。また、正常であることがわかっている最新のマスタ ブート レコードを復元する	コンピュータ セットアップ ユーティリティ (F10) メニューを使う
メモリ脱着センサ (Memory Change Alerts)	メモリの脱着があったことを知らせる	設定方法などについては、オンライン ヘルプの「インテリジェント マネジメント機能」の説明を参照
オーナーシップ タグ (Ownership Tag)	コンピュータの起動時に所有者に関する情報を画面に表示する	コンピュータ セットアップ ユーティリティ (F10) メニューを使う
ケーブル ロック (Cable Lock Provision)	南京錠でコンピュータ本体のカバーを施錠して、コンピュータの設定を変更したり内部装置を取り外したりできないようにする 盗難防止ケーブルでコンピュータを固定して、無断で持ち出せないようにする セキュリティ ブラケットに南京錠を取り付けて、机などに固定する	セキュリティ ブラケットに市販の盗難防止ケーブルを取り付ける
セキュリティ ループ (Security Loop Provision)	コンピュータの設定を変更したり内部装置を取り外したりできないようにする	セキュリティ ループに錠を取り付け、コンピュータの設定を変更したり内部装置を取り外したりできないようにする
 コンピュータ セットアップについて詳しくは、『コンピュータ セットアップ (F10) ユーティリティ ガイド』を参照してください。サポートされるセキュリティ機能は、お使いのコンピュータの構成によって異なる場合があります。		

## パスワードのセキュリティ

電源投入時パスワードは、コンピュータの電源を入れたり再起動するたびに、アプリケーションやデータにアクセスするためのパスワードの入力が要求されるので、コンピュータが許可無く使用されることを防ぎます。セットアップパスワードは、特にコンピュータ セットアップ ユーティリティへの不正アクセスを防ぎます。セットアップパスワードを、電源投入時パスワードの補助手段として使用することもできます。つまり、電源投入時パスワードの入力を要求されたときに、代わりにセットアップパスワードを入力してコンピュータにアクセスすることもできます。

ネットワーク全体のセットアップパスワードを設定しておく、システム管理者はネットワーク上のすべてのシステムにログインでき、設定されている電源投入時パスワードを知らなくてもメンテナンスを行うことができます。

### セットアップ パスワード (Setup Password) の設定

[コンピュータ セットアップ (F10) ユーティリティ]メニューで、セットアップパスワードを設定しておけば、無断でコンピュータの設定を変更されるのを防ぐことができます。

1. コンピュータの電源を入れるか、再起動します。

Windows 2000をお使いの場合、[スタート]→[シャットダウン]→[再起動]→[OK]の順に選択します。

Windows XPをお使いの場合、[スタート]→[終了オプション]→[再起動]の順に選択します。

2. HPのロゴ画面の右下に[F10=Setup]と表示されたら、すぐに[F10]キーを押します。必要であれば、[Enter]キーを押してタイトル画面を終了してください。



画面右下に[F10=Setup]と表示されている間に[F10]キーを押せなかったときは、コンピュータを再起動して操作をやりなおしてください。

3. [セキュリティ] (Security) → [セットアップ パスワード] (Setup Password) の順に選択したあと、画面上のメッセージに従って操作します。
4. 設定を終了するには、[ファイル] (File) → [変更を保存して終了] (Save Changes and Exit) の順に選択します。

## 電源投入時パスワード（Power-On Password）の設定

[コンピュータ セットアップ ユーティリティ]メニューで、電源投入時パスワードを設定しておけば、無断でコンピュータが使用されることを防止できます。電源投入時パスワードが設定されていると、コンピュータ セットアップ ユーティリティの[Security]（セキュリティ設定）メニューに[Password options]（パスワード オプション）が表示されます。パスワード オプションには[Network Server Mode]（ネットワーク サーバ モード）と[Password Prompt on Warm Boot]（ウォーム ブート時のパスワード入力）が含まれます。

ネットワーク サーバ モード（Network Server Mode）が無効（Disable）にされている場合は、コンピュータに電源を入れるたびに、鍵型のアイコンがモニタに表示されるのでパスワードを正しく入力しなしてください。[Password Prompt on Warm Boot]（ウォーム ブート時のパスワード入力）が有効にされている場合も、コンピュータを再起動するたびにパスワードを入力する必要があります。[Network Server Mode]（ネットワーク サーバ モード）が有効（Enable）にされていると、POSTの実行中にパスワードは要求されませんが、ユーザが電源投入時パスワードを入力するまで、接続されているPS/2キーボードはロックされたままです。

1. コンピュータの電源を入れるか、再起動します。

Windows 2000をお使いの場合、[スタート]→[シャットダウン]→[再起動]→[OK]の順に選択します。

Windows XPをお使いの場合、[スタート]→[終了オプション]→[再起動]の順に選択します。

2. HPのロゴ画面の右下に[F10=Setup]と表示されたら、すぐに[F10]キーを押します。必要であれば、[Enter]キーを押してタイトル画面を終了してください。



画面右下に[F10=Setup]と表示されている間に[F10]キーを押せなかったときは、コンピュータを再起動して操作をやりなおしてください。

3. [セキュリティ]→[電源投入時パスワード]（Power-On Password）の順に選択したあと、画面上のメッセージに従って操作します。
4. 設定を終了するには、[ファイル]→[変更を保存して終了]の順に選択します。



## 電源投入時パスワード（Power-On Password）の入力

電源投入時パスワードを入力するには、次の手順で行います。

1. コンピュータの電源を入れるか、再起動します。  
Windows 2000をお使いの場合、[スタート]→[シャットダウン]→[再起動]→[OK]の順に選択します。  
Windows XPをお使いの場合、[スタート]→[終了オプション]→[再起動]の順に選択します。
2. 鍵形のアイコンが表示されたら、パスワードを入力して[Enter]キーを押します。



機密保護のため、入力したパスワードは画面に表示されません。パスワードを入力する際は、間違えないよう注意してください。

間違ったパスワードを入力した場合は、鍵形に×印のついたアイコンが表示されますので、パスワードを正しく入力しなおしてください。続けて3回間違えた場合は、コンピュータの電源をいったん切って最初からやりなおさなければなりません。

## セットアップ パスワード（Setup Password）の入力

コンピュータで、セットアップ パスワードを設定しておけば、[コンピュータ セットアップ ユーティリティ]メニューを実行するたびに、必ずパスワードの入力が必要となります。

1. コンピュータの電源を入れるか、再起動します。  
Windows 2000をお使いの場合、[スタート]→[シャットダウン]→[再起動]→[OK]の順に選択します。  
Windows XPをお使いの場合、[スタート]→[終了オプション]→[再起動]の順に選択します。
2. HPのロゴ画面の右下に[F10=Setup]と表示されたら、すぐに[F10]キーを押します。



画面右下に[F10=Setup]と表示されている間に[F10]キーを押せなかったときは、コンピュータを再起動して操作をやりなおしてください。

3. 鍵形のアイコンが表示されたら、セットアップ パスワードを入力して[Enter]キーを押します。



機密保護のため、入力したパスワードは画面に表示されません。パスワードを入力する際は、間違えないよう注意してください。

---

間違ったパスワードを入力した場合は、鍵形に×印のついたアイコンが表示されますので、パスワードを正しく入力しなおしてください。続けて3回間違えた場合は、コンピュータの電源をいったん切ってからやりなおさなければなりません。

## 電源投入時パスワード（Power-On Password）/セットアップパスワード（Setup Password）の変更

次の手順で電源投入時パスワードを変更します。

1. コンピュータの電源を入れるか、再起動します。

Windows 2000をお使いの場合、[スタート]→[シャットダウン]→[再起動]→[OK]の順に選択します。

Windows XPをお使いの場合、[スタート]→[終了オプション]→[再起動]の順に選択します。

2. 鍵形のアイコンが表示されたら、次のように入力します。

現在のパスワード/新しいパスワード/新しいパスワード



機密保護のため、タイプしたパスワードは画面に表示されません。パスワードを入力する際は、間違えないよう注意してください。

---

3. [Enter]キーを押します。

新しいパスワードは、次にコンピュータの電源を入れたときから有効になります。



電源投入時パスワードとセットアップパスワードは、コンピュータ セットアップ ユーティリティのセキュリティ（Security）オプションを使って変更することもできます。

---

## 電源投入時パスワード（Power-On Password）/セットアップ パスワード（Setup Password）の削除

パスワードを削除するには、次の手順で行います。

1. コンピュータの電源を入れるか、再起動します。

Windows 2000をお使いの場合、[スタート]→[シャットダウン]→[再起動]→[OK]の順に選択します。

Windows XPをお使いの場合、[スタート]→[終了オプション]→[再起動]の順に選択します。

2. 鍵形のアイコンが表示されたら、次のようにタイプします。

現在のパスワード/

3. [Enter]キーを押します。



電源投入時パスワードとセットアップパスワードは、コンピュータ セットアップ ユーティリティのセキュリティ（Security）オプションを使って変更することもできます。

## 電源投入時パスワード（Power-On Password）を忘れてしまった場合

設定しておいた電源投入時パスワードを忘れると、コンピュータを使用できなくなります。パスワードを解除する方法については、『トラブルシューティング ガイド』を参照してください。

## ネットワーク サーバ モード

ネットワーク サーバ モードによって、サーバとして使用するコンピュータに独自のセキュリティ機能が提供されます。この機能は、コンピュータ セットアップ ユーティリティで電源投入時パスワードが設定された場合にのみ有効です。ネットワーク サーバ モードが有効になっていると、ハードディスクドライブからのブート時に電源投入時パスワードを入力する必要がなくなり、キーボードをシステムに接続する必要もなくなります。PS/2 キーボードが接続されている場合は、ユーザが電源投入時パスワードを入力するまでロックされます。USB キーボードが接続されている場合は、特に指定しないかぎり、使用可能のままになります。オペレーティング システムが読み込まれた後にUSB キーボードからアクセスされないようにするには、コンピュータ セットアップ ユーティリティを使用して、**[Security]** (セキュリティ設定) メニューの **[Device security]** (デバイス セキュリティ) で、USB ポートを非表示にする必要があります。ネットワーク サーバ モードを、コンピュータ セットアップ ユーティリティの**[電源の切断後]** (After Power Loss) 電源オプションと組み合わせて使用すると、停電解消後、ユーザが操作をすることなく、サーバによって自動的に再起動されます。ネットワーク サーバ モードが有効になっている場合、リムーバブル メディア (ディスクなど) やリムーバブル デバイス (USB フラッシュ デバイスなど) からブートするときは、電源投入時パスワードを入力する必要があります。

## ドライブロック

ドライブロックは、特定のハードディスク ドライブにあるデータへの不正アクセスを禁止するセキュリティ機能であり、コンピュータ セットアップ ユーティリティの拡張機能として実装されています。この機能は、一部のシステムでのみ、さらに、ドライブロックが可能なハードディスク ドライブが検出された場合にのみ、利用できます。

ドライブロックは、データのセキュリティを最重要視するユーザ向けに開発されました。このようなユーザにとっては、ハードディスク ドライブのコストとそこに格納されているデータの喪失は、データへの不正アクセスの結果生じる可能性のある損害に比べれば、些細なものです。このレベルのセキュリティを確保すると同時に、パスワードを忘れたときの対処もできるように、ドライブロックでは、2つのパスワードによるセキュリティ方式を採用しています。一方のパスワードはシステム管理者が設定し、使用するもので、もう一方のパスワードは通常、エンドユーザが設定し、使用します。両方のパスワードを忘れてしまった場合にドライブをアンロックするための手段はありません。したがって、ハードディスク ドライブに含まれるデータが企業情報システムに複製されているか、または定期的にバックアップが作成されている場合に、ドライブロックを最も安全に使用できます。

ドライブロックの両方のパスワードを忘れてしまった場合は、ハードディスク ドライブを使用できなくなります。事前に定義されたカスタマー プロファイルに適合しないすべてのユーザにとって、この事実は受け入れ難いリスクになる可能性があります。一方、カスタマー プロファイルに適合するユーザにとっては、ハードディスク ドライブに保存されたデータの性質上、許容できるリスクだと言えます。

## ドライブロックの使用法

[DriveLock]（ドライブロック）オプションは、コンピュータ セットアップ ユーティリティの[Security]（セキュリティ設定）メニューに表示されます。ユーザには、マスタ パスワードを設定したりドライブロックを有効にするオプションが提供されます。ドライブロックを有効にするには、ユーザのパスワードを入力する必要があります。通常、ドライブロックの最初のコンフィギュレーションはシステム管理者が実行するので、マスタ パスワードが最初に設定されます。ドライブロックを有効にするか無効のままにしておくかにかかわらず、管理者はマスタ パスワードを設定することをお勧めします。これにより、将来ドライブがロックされた場合に、管理者はドライブロックの設定値を変更できるようになります。マスタ パスワードが設定されると、システム管理者はいつでもドライブロックを有効にしたり無効にしたりすることができます。

ロックされたハードディスク ドライブが存在する場合は、POST（Power-On Self Test）によって、そのドライブをアンロックするためのパスワードが要求されます。電源投入時パスワードが設定されていて、また、そのドライブのユーザ パスワードと一致する場合は、パスワードの再入力には要求されません。一致しない場合は、ドライブロックのパスワードを入力するよう要求されます。マスタ パスワードとユーザ パスワードのどちらを使うこともできます。ユーザは、パスワードが正しいと認められるまで、2回入力できます。2回とも受け入れられない場合でもPOSTは続行されますが、そのドライブのデータにはアクセスできません。

## ドライブロックの使用例

ドライブロックのセキュリティ機能は、企業環境での使用に最も適しています。つまり、システム管理者が、ユーザに複数のコンピュータで使用できるようマルチベイ ハードディスク ドライブを提供する場合です。システム管理者はマルチベイ ハードディスク ドライブのコンフィギュレーションを担当しますが、その中で最も重要な作業は、ドライブロックのマスタ パスワードを設定することです。ユーザがユーザ パスワードを忘れたり、コンピュータを別の従業員が使うようになった場合、システム管理者はマスタ パスワードを使用して、ユーザ パスワードをリセットしたり、ハードディスク ドライブへのアクセス権を回復したりすることができます。


企業システム管理者は、ドライブロックを有効にする場合、マスタ パスワードの設定とメンテナンスについての企業方針を確立しておくことをお勧めします。こうすることで、従業員が会社を辞める前に意図的に、または誤ってドライブロックの両方のパスワードを設定してしまうという状況を防ぐことができます。両方のパスワードを設定した従業員が会社を辞めてしまった場合、そのハードディスク ドライブは使用不能となり、交換が必要になります。また、マスタ パスワードが設定されていないと、システム管理者がロックされたハードディスク ドライブにアクセスできなくなり、不正ソフトウェアの日常チェックや、その他の資産管理およびサポートを実行できなくなることがあります。

それほど嚴重なセキュリティは必要としないユーザの場合は、ドライブロックを有効にしないことをお勧めします。この種のユーザには、個人ユーザや、機密性の高いデータをハードディスク ドライブに保持しないことを習慣にしているユーザが含まれます。このようなユーザにとっては、両方のパスワードを忘れてハードディスク ドライブ上のデータを失うことの損失のほうが、データを保護するために設計されたドライブロックの価値よりもはるかに大きいといえます。コンピュータ セットアップ ユーティリティとドライブロックへのアクセスは、セットアップ パスワードによって制限できます。セットアップ パスワードを指定してそれをエンド ユーザに公表しないことで、システム管理者はユーザがドライブロックを有効にできないようにします。

## スマート カバー センサ / カバー リムーバブル センサ (Cover Removable Sensor)

一部のモデルに搭載されているスマート カバー センサ/カバー リムーバブル センサとは、本体のカバーまたはサイドパネルの脱着があったことをユーザに知らせるハードウェア技術とソフトウェア技術を結合した機能です。3段階の設定レベルがあり、本体のカバーの脱着があった後はじめてコンピュータの電源を入れたときの動作が異なります。

### スマート カバー センサ/カバー リムーバブル センサの動作

レベル	設定	コンピュータ起動時の動作
0	[Disabled] (無効)	(スマート カバー センサ/カバー リムーバブル センサは無効)
1	[Notify User] (ユーザに通知)	本体のカバーが取り外されたことを知らせるメッセージが画面に表示される
2	[Setup Password] (セットアップ パスワード)	本体のカバーが取り外されたことを知らせるメッセージが画面に表示される。 セットアップ パスワードを入力するまで、コンピュータを使用できない
 これらの設定は、コンピュータ セットアップを使用して変更できます。コンピュータ セットアップについて詳しくは、『コンピュータ セットアップ ユーティリティ (F10) ガイド』を参照してください。		



## スマート カバー センサ/カバー リムーバブル センサ (Cover Removable Sensor) の設定

次の手順で、スマート カバー センサ/カバー リムーバブル センサ機能を有効にします。

1. コンピュータの電源を入れるか、再起動します。

Windows 2000をお使いの場合、[スタート]→[シャットダウン]→[再起動]→[OK]の順に選択します。

Windows XPをお使いの場合、[スタート]→[終了オプション]→[再起動]の順に選択します。

2. HPのロゴ画面の右下に[F10=Setup]と表示されたら、すぐに[F10]キーを押します。必要であれば、[Enter]キーを押してタイトル画面を終了してください。



画面右下に[F10=Setup]と表示されている間に[F10]キーを押せなかったときは、コンピュータを再起動して操作をやりなおしてください。

3. [セキュリティ]→[スマート カバー]の順に選択したあと、画面上に表示されている項目より選択します。
4. 設定を終了するには、[ファイル]→[変更を保存して終了]の順に選択します。

## スマート カバー ロック (Smart Cover Lock)

スマート カバー ロックは、一部のHPのコンピュータでサポートされるコンピュータのカバーのロックをソフトウェアで制御する機能です。スマート カバー ロックを使用して、コンピュータ内部の装置への不正なアクセスを防ぎます。工場出荷時には、ロックが解除された状態となっています。



**注意:** スマート カバー ロックを使用する場合は、必ずセットアップパスワードを設定して、無断でロックを解除できないようにしておいてください。



スマート カバー ロックは、一部のシステムにオプションとして装備されています。

## スマート カバー ロック (Smart Cover Lock) の設定

次の手順で、スマート カバー ロックを使って、コンピュータ本体のカバーをロックします。

1. コンピュータの電源を入れるか、再起動します。  
Windows 2000をお使いの場合、[スタート]→[シャットダウン]→[再起動]→[OK]の順に選択します。  
Windows XPをお使いの場合、[スタート]→[終了オプション]→[再起動]の順に選択します。
2. HPのロゴ画面の右下に[F10=Setup]と表示されたら、すぐに[F10]キーを押します。必要であれば、[Enter]キーを押してタイトル画面を終了してください。



---

画面右下に[F10=Setup]と表示されている間に[F10]キーを押せなかったときは、コンピュータを再起動して操作をやりなおしてください。

---

3. [セキュリティ]→[スマート カバー]→[カバー ロック] (Cover Lock) →[ロック] (Lock) の順に選択します。
4. 設定を終了するには、[ファイル]→[変更を保存して終了] の順に選択します。

## スマート カバー ロック (Smart Cover Lock) の解除

1. コンピュータの電源を入れるか、再起動します。  
Windows 2000をお使いの場合、[スタート]→[シャットダウン]→[再起動]→[OK]の順に選択します。  
Windows XPをお使いの場合、[スタート]→[終了オプション]→[再起動]の順に選択します。
2. HPのロゴ画面の右下に[F10=Setup]と表示されたら、すぐに[F10]キーを押します。必要であれば、[Enter]キーを押してタイトル画面を終了してください。



---

画面右下に[F10=Setup]と表示されている間に[F10]キーを押せなかったときは、コンピュータを再起動して操作をやりなおしてください。

---

3. [セキュリティ]→[スマート カバー]→[アンロック] (UnLock) オプションの順に選択します。
4. 設定を終了するには、[ファイル]→[変更を保存して終了] の順に選択します。

## Smart Cover FailSafeキーの使用

スマート カバー ロックを使ってコンピュータをロックしたまま、パスワードを入力できなくなってしまった場合、Smart Cover FailSafeキーを使用して、コンピュータ本体のカバーを開ける必要があります。Smart Cover FailSafeキーが必要となるのは、次のような場合です。

- 停電
- 起動障害
- コンピュータ部品（プロセッサや電源など）障害
- パスワードを忘れてしまった場合



**注意：** Smart Cover FailSafeキーは、HPが提供する専用ツールです。必要になる前に、HP製品販売店であらかじめご用意いただくことをおすすめします。

Smart Cover FailSafeキーの入手については、HPのサポート窓口にお問い合わせください。

Smart Cover FailSafeキーについて詳しくは、『ハードウェア リファレンス ガイド』を参照してください。

## マスタ ブート レコード セキュリティ (Master Boot Record Security)

マスタ ブート レコード (MBR) には、ディスクから正常に起動して、ディスク上に保存されているデータにアクセスするための情報が入っています。マスタ ブート レコードのセキュリティ機能によって、誤ってMBRを変更したり不正にMBRが変更される（一部のコンピュータ ウイルスによってデータが変更されたり、ディスク ユーティリティを誤って使用するなど）のを防ぐことができます。また、システムの再起動時にMBRへの変更が検出された場合、このセキュリティによって「正常であることが分かっている最新の」MBRを復元することができます。

MBRセキュリティを有効にするには、次の手順で行います。

1. コンピュータの電源を入れるか、再起動します。  
Windows 2000をお使いの場合、[スタート]→[シャットダウン]→[再起動]  
→[OK]の順に選択します。  
Windows XPをお使いの場合、[スタート]→[終了オプション]→[再起動]の  
順に選択します。
2. 画面右下に[F10=Setup]と表示されたら、すぐに[F10]キーを押します。必  
要であれば、[Enter]キーを押してタイトル画面を終了してください。



画面右下に[F10=Setup]と表示されている間に[F10]キーを押せなかったとき  
は、コンピュータを再起動して操作をやりなおしてください。

---

3. [セキュリティ]→[マスタ ブート レコード セキュリティ] (Master Boot  
Record Security) →[有効] (Enabled) の順に選択します。
4. [セキュリティ]→[マスタ ブート レコードの保存] (Save Master Boot  
Record) の順に選択します。
5. 設定を終了するには、[ファイル]→[変更を保存して終了]の順に選択しま  
す。

MBRセキュリティを有効にすると、BIOSは、MS-DOSやWindowsのSafeモー  
ドで現在の起動可能ディスクのMBRが変更されることを防ぎます。



ほとんどのオペレーティング システムは、現在の起動可能ディスクのMBRへ  
のアクセスを制御します。したがって、オペレーティング システムの動作中  
に行われる変更については、BIOSは阻止できません。

---

コンピュータの電源を入れるか、再起動するたびに、BIOSは現在の起動可能  
ディスクのMBRと前回に保存されたMBRとを比較します。変更が検出され、  
かつ現在の起動可能ディスクが、前回MBRを保存したディスクと同じである  
場合、次のメッセージが表示されます。

1999 - Master Boot Record has changed. (マスタ ブート レコードが変更されま  
した。)

Press any key to enter Setup to configure MBR Security (任意のキーを押して[コ  
ンピュータ セットアップ ユーティリティ]メニューで、MBRセキュリティを  
設定してください。)

[コンピュータ セットアップ ユーティリティ]メニューで、次の操作を行います。

- 現在の起動可能ディスクのMBRを保存します。
- 前回保存したMBRを復元します。または、
- MBRセキュリティ機能を無効にします。

セットアップ パスワードが設定されている場合は、セットアップ パスワードの入力が必要です。

変更が検出され、現在の起動可能ディスクが、前回にMBRを保存したディスクと同じでない場合は、次のメッセージが表示されます。

2000 - Master Boot Record Hard Drive has changed. (マスタ ブート レコードのハードディスク ドライブが変更されています。)

Press any key to enter Setup to configure MBR Security (任意のキーを押して[コンピュータ セットアップ ユーティリティ]メニューで、MBRセキュリティを設定してください。)

[コンピュータ セットアップ ユーティリティ]メニューで、次の操作を行います。

- 現在の起動可能ディスクのMBRを保存します。または、
- MBRセキュリティ機能を無効にします。

セットアップ パスワードが設定されている場合は、セットアップ パスワードの入力が必要です。

万一、前回保存したMBRが破損した場合は、次のメッセージが表示されます。

1998 - Master Boot Record has been lost. (マスタ ブート レコードがありません。)

Press any key to enter Setup to configure MBR Security (任意のキーを押して[コンピュータ セットアップ ユーティリティ]メニューで、MBRセキュリティを設定してください。)

[コンピュータ セットアップ ユーティリティ]メニューで、次の操作を行います。

- 現在の起動可能ディスクのMBRを保存します。または、
- MBRセキュリティ機能を無効にします。

セットアップ パスワードが設定されている場合は、セットアップ パスワードの入力が必要です。

### 現在の起動可能ディスクのパーティションとフォーマットを変更する前に

現在の起動可能ディスクのパーティションやフォーマットを変更する前に、MBRセキュリティが無効になっていることを確認してください。FDISKやFORMATなど一部のディスク ユーティリティは、MBRを更新しようとする。ディスクのパーティションやフォーマットを変更する際にMBRセキュリティが有効である場合は、次にコンピュータの電源を入れるか再起動したときに、ディスク ユーティリティからエラー メッセージが表示されたり、MBRセキュリティから警告が発生する可能性があります。MBRセキュリティを無効にするには、次の手順で行います。

1. コンピュータの電源を入れるか、再起動します。  
Windows 2000をお使いの場合、[スタート]→[シャットダウン]→[再起動]→[OK]の順に選択します。  
Windows XPをお使いの場合、[スタート]→[終了オプション]→[再起動]の順に選択します。
2. 画面右下に[F10=Setup]と表示されたら、すぐに[F10]キーを押します。必要であれば、[Enter]キーを押してタイトル画面を終了してください。



画面右下に[F10=Setup]と表示されている間に[F10]キーを押せなかったときは、コンピュータを再起動して操作をやりなおしてください。

3. [セキュリティ]→[マスタ ブート レコード セキュリティ]→[無効] (Disabled)の順に選択します。
4. 設定を終了するには、[ファイル]→[変更を保存して終了]の順に選択します。

## ケーブル ロックの取り付け

コンピュータのリア パネルにはケーブル ロックを取り付けられるようになっているので、市販のケーブル ロックを使用して、コンピュータを作業エリアに固定できます。

詳細については、Documentation Library CDに収録されている『ハードウェア リファレンス ガイド』を参照してください。

## 指紋認証テクノロジー

HP 指紋認証テクノロジーを使用すると、エンド ユーザのパスワードの入力が不要となるため、ネットワークのセキュリティを強化する一方で、ログイン手順を簡素化し、企業のネットワーク管理に関わる経費を削減することができます。また、価格もリーズナブルであるため、もはや一部のハイテク産業やハイ レベルのセキュリティを扱う組織や企業だけのものではなくなりました。



指紋認証テクノロジーは、サポートされているモデルとサポートされていないモデルがあります。

詳しくは、[http://www.compaq.com/products/quickspecs/10690\\_na/10690\\_na.html](http://www.compaq.com/products/quickspecs/10690_na/10690_na.html) (英語サイト) を参照してください。

## 障害通知および復旧機能

障害通知および復旧機能とは、最新のハードウェア/ソフトウェア技術を結合して、重要なデータの損失を防ぎ、故障時間を最小限に抑える機能で、障害が発生すると、障害内容と対処方法を示した警告メッセージを画面上に表示します。また、HP Insight マネジメント エージェントを使用すれば、いつでもシステムの状態を調べることができます。HP Insight マネージャ製品またはコンパック マネジメント ソリューションのパートナー企業が提供する他のネットワーク管理ソフトウェアによって管理されるネットワークにコンピュータが接続されている場合は、ネットワーク管理ソフトウェアにも障害通知が送られます。

## ドライブ保護システム

ドライブ保護システム（DPS）は、一部のモデルに搭載されたコンピュータのハードディスク ドライブに組み込まれている診断ツールです。DPSを使用して、ハードディスクの交換時に発生する問題を診断します。

コンピュータにハードディスク ドライブを取り付ける際にDPSテストを実行し、主要な情報をハードディスク ドライブに書き込みます。この情報は半永久的に記録されます。DPSを実行するたびに、テストの結果がハードディスク ドライブに書き込まれます。HP 正規保守代理店はこの情報を使用して問題の原因を診断します。DPSの使用手順については『トラブルシューティング ガイド』を参照してください。

## Ultra ATA監視機能

Ultra ATA 監視機能は、Ultra ATA ハードディスク ドライブとシステム上の回路との間で送受されたデータを監視し、エラーを検出すると、障害内容を示した警告メッセージをコンピュータの画面上に表示します。

## 耐サージ機能付連続供給電源装置

耐サージ機能が付いた連続供給電源によって、急激な電圧の変化に対処することができます。この電源装置は、2000 ボルトまでのサージ電圧に耐えて、データの損失やシステム ダウンを引き起こさないことが確認されています。

## 温度センサ機能

温度センサ機能は、ハードウェアとソフトウェアの統合により提供される機能で、コンピュータ内部の温度を監視し、コンピュータ内部の温度が通常の範囲を超えると、画面上に警告メッセージを表示します。これにより、内部部品の故障やデータの損失が発生する前に対処することができます。



モデルにより温度センサ機能はサポートされない場合があります。

---



# 索引

<b>A</b>			
ActiveUpdate	8	変更	13
Altiris eXpress	4, 6	温度、コンピュータ内部	36
Altiris eXpress HP/Compaq Client Manager	6	温度センサ機能	36
Altiris eXpress PC Transplant Pro	6		
<b>F</b>		<b>か</b>	
FailSafeキー		カバー ロック、スマート	29
注意	31	カバー ロックの安全、注意	29
<b>P</b>		キーボード ランプ、ROM	11
PCN（製品変更通知）	7	ケーブル ロックの取り付け	35
<b>R</b>		コンピュータ セットアップ ユーティティ	11
ROMの保護、注意	8	コンピュータ内部の温度	36
ROM、無効	9	コンフィギュレーション電源ボタン	12
<b>S</b>		<b>さ</b>	
SSM（System Software Manager）	7	資産情報管理機能	15
System Software Manager（SSM）	7	システムの復旧	9
<b>U</b>		指紋認証テクノロジー	35
Ultra ATA監視機能	36	重要な情報	
URL（Webサイト）		ディスクのパーティション	34
「Webサイト」を参照		ディスクのフォーマット	34
<b>W</b>		ブート可能ディスク	34
Webサイト		出荷時の設定	2
www.compaq.com/activeupdate	8	障害通知	35
www.compaq.com/easydeploy	5, 14	省電力機能	13
www.compaq.com/im	7	スマート カバー ロック	
www.compaq.com/products/quickspecs/10690_na/10690_na.html	35	解除	30
www.compaq.com/solutions/pcsolutions/	2	製品変更通知（PCN）	7
www.compaq.com/pcn、PCN	7	セキュリティ、マスタ ブート レコード	31
WWWアドレス		設定	
「Webサイト」を参照		スマート カバー センサ/カバー リムーバブル	
<b>あ</b>		センサ	29
インターネットのホームページ		セットアップ パスワード	19
「Webサイト」を参照		タイムアウト	13
インテリジェント マネジメント機能	14	マスタ ブート レコードセキュリティ	32
オペレーティング システム		セットアップ	
重要な情報	13	初期設定	2
		パスワード	19
		削除	23
		入力	21
		変更	22
		リプリーケート機能	11

ソフトウェア		ドライブ、保護	36
Altiris eXpress	4	な	
System Software Manager	7	入力	
コンピュータ セットアップ ユーティリティ	11	セットアップ パスワード	21
資産情報管理機能	15	電源投入時パスワード	21
障害通知および復旧機能	35	は	
省電力機能	13	ハードディスク ドライブ診断ツール	36
統合	2	ハードディスク ドライブの保護	36
ドライブ保護システム	36	パスワード	
ブート ブロックROM	10	削除	23
複数のコンピュータをアップデート	7	セットアップ	19, 21
マスタ ブート レコード セキュリティ	31	電源投入時	21
リストア	2	変更	22
リモートROMフラッシュ	9	忘れた場合	23
リモート システム インストール	3	表	
た		ROMによるキーボード ランプ	11
耐サージ機能付連続供給電源装置	36	スマート カバー センサ/カバー リムーバブル	
タイムアウト	13	センサの動作	28
注意		セキュリティ機能	17
FailSafeキー	31	ブート ブロックROM	10
ROMの保護	8	複製ツール、ソフトウェア	2
カバー ロックの安全	29	プリインストールされたソフトウェア イメージ	2
ディスク、複製	2	ま	
データ機能	36	無効のシステム	9
デュアル ステート電源ボタン	12	ら	
電源供給、耐サージ機能	36	リストア、ソフトウェア	2
電源投入時パスワード		リモート	
削除	23	ROMフラッシュ	9
入力	21	システム インストール、アクセス	3
変更	22	セットアップ	3
電源ボタン		わ	
コンフィギュレーション	12	忘れた場合	
デュアル ステート	12	パスワード	23
導入用ツール、ソフトウェア	2		